A SCHEME FOR DEVICE AND USER AUTHENTICATION WITH KEY DISTRIBUTION IN A WIRELESS NETWORK

ABSTRACT OF THE INVENTION

In a computer network, a method of mutually authenticating a client device and a network interface, authenticating a user to the network and exchanging encryption keys. In one embodiment, the method comprises authenticating the client device at the local network device point, with which the client device exchanges an encryption key and then the user is authenticated by a central authentication server. In another embodiment, the method comprises authenticating the client device at the central authentication server, with which the client device exchanges a key which is passed to the network device with a secret shared between the central authentication server and the network device. In this embodiment, the user is also authenticated at the central authentication server.